CLAIMS

What is claimed is:

1. A secure hard drive, comprising:

a storage medium that stores encrypted digital content and corresponding encrypted content keys;

a public key decryption module that receives one of said encrypted content keys from said storage medium and that decrypts said encrypted content key using a private key and generates a content key; and

a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key.

2. The secure hard drive of Claim 1 wherein said storage medium is a magnetic storage medium.

3. The secure hard drive of Claim 1 wherein said public key decryption module and said block decryption module are implemented by a system on chip (SOC).

4. The secure hard drive of Claim 1 further comprising:

a content player that receives said decrypted digital content from said block decryption module and that generates at least one of an analog output signal and a digital output signal; and

an identification (ID) module that provides an ID, wherein said private key and a public key are based on said ID.

5. The secure hard drive of Claim 1 further comprising a controller that performs buffer management and timing of read/write operations.

6. A system comprising the secure hard drive of Claim 5 and further comprising:

an external host; and

a control interface that provides a communications interface between said controller and said external host.

7. The system of Claim 6 wherein said external host is one of a computer and a portable media player.

8. The secure hard drive of Claim 4 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark.

9. The secure hard drive of Claim 1 wherein said storage medium stores a content directory having content directory entries for said content.

10. The secure hard drive of Claim 9 wherein said public key decryption module performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

11. The secure hard drive of Claim 9 wherein at least one of said content directory entries contains a clear content counter that specifies a portion of said corresponding content that is not encrypted.

12. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content distributor identification (ID) field that identifies a content distributor supplying said corresponding content.

13. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback.

14. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

15. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storage medium.

16. The secure hard drive of Claim 9 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storage medium.

17. The secure hard drive of Claim 1 wherein said content includes at least one of audio, video, and still pictures.

18. The system of Claim 6 further comprising:

a distributed communications network; and

a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications network.

19. The secure hard drive of Claim 1 wherein said storage medium contains encrypted content that is pre-stored thereon.

20. A secure hard drive, comprising:

a magnetic storage medium that stores encrypted digital content and corresponding encrypted content keys;

a system on chip (SOC) including:

a public key decryption module that receives one of said encrypted content keys from said magnetic storage medium and that decrypts said encrypted content key using a private key of said SOC to generate a content key; and

a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said magnetic storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key.

21. The secure hard drive of Claim 20 further comprising a content player that receives said decrypted digital content from said block decryption module and that generates an analog output signal.

22. The secure hard drive of Claim 20 further comprising a chip identification (ID) module that provides a chip ID for said SOC, wherein said private key and a public key of said SOC are based on said chip ID.

23. The secure hard drive of Claim 20 wherein said SOC further includes a controller that performs buffer management and timing of read/write operations.

24. A system comprising the secure hard drive of Claim 23 and further comprising:

an external host; and

a control interface that provides an interface between said controller and said external host.

25. The secure hard drive of Claim 21 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark.

26. The secure hard drive of Claim 20 wherein said magnetic storage medium stores a content directory having content directory entries for said content.

27. The secure hard drive of Claim 26 wherein said public key decryption module performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

28. The secure hard drive of Claim 26 wherein at least one of said content directory entries contains at least one of a clear content counter that specifies a portion of said corresponding content that is not encrypted, a content distributor identification (ID) field that identifies a content distributor supplying said corresponding content, a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback, a signature field for said content distributor supplying said corresponding content, a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said magnetic storage medium, and a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said magnetic storage medium.

29. The secure hard drive of Claim 20 wherein said content includes at least one of audio, video, and still pictures.

30. The system of Claim 24 further comprising:

a distributed communications network; and

a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications system.

31. A secure hard drive, comprising:

storing means for storing encrypted digital content and corresponding encrypted content keys;

public key decryption means for receiving one of said encrypted content keys from said storing means and for decrypting said encrypted content key using a private key to generate a content key; and

block decryption means for receiving said encrypted digital content corresponding to said one of said encrypted content keys from said storing means and said content key from said public key decryption means and for decrypting said encrypted content using said content key.

32. The secure hard drive of Claim 31 wherein said storing means includes a magnetic storing medium.

33. The secure hard drive of Claim 31 wherein said public key decryption means and said block decryption means are implemented by a system on chip (SOC).

34. The secure hard drive of Claim 31 further comprising:

content playing means for receiving said decrypted digital content from said block decryption means and for generating at least one of an analog output signal and a digital output signal; and

identification (ID) means for providing an ID, wherein said private key and a public key are based on said ID.

35. The secure hard drive of Claim 31 further comprising controller means for performing buffer management and timing of read/write operations.

36. A system comprising the secure hard drive of Claim 35 and further comprising:

an external host; and

control interface means for providing a communications interface between said controller means and said external host.

37. The system of Claim 36 wherein said external host is one of a computer and a portable media player.

38. The secure hard drive of Claim 34 further comprising watermark detecting means that communicates with an output of said content playing means for determining whether said analog signal that is output by said content playing means contains a watermark.

39. The secure hard drive of Claim 31 wherein said storing means stores a content directory having content directory entries for said content.

40. The secure hard drive of Claim 39 wherein said public key decryption means performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

41. The secure hard drive of Claim 39 wherein at least one of said content directory entries contains clear content counting means for specifying a portion of said corresponding content that is not encrypted.

42. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content distributor identification (ID) field that identifies a content distributor supplying said corresponding content.

43. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback.

44. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

45. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storing means.

46. The secure hard drive of Claim 39 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storing means.

47. The secure hard drive of Claim 31 wherein said content includes at least one of audio, video, and still pictures.

48. The system of Claim 36 further comprising:

distributed means for providing a distributed communications network; and

content distributor means for transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed means.

49. The secure hard drive of Claim 31 wherein said storing means contains encrypted content that is pre-stored thereon.

50. A secure hard drive, comprising:

magnetic storing means that stores encrypted digital content and corresponding encrypted content keys;

a system on chip (SOC) including:

public key decryption means for receiving one of said encrypted content keys from said magnetic storage means and for decrypting said encrypted content key using a private key of said SOC to generate a content key; and

block decryption means for receiving said encrypted digital content corresponding to said one of said encrypted content keys from said magnetic storing means and said content key from said public key decryption means and for decrypting said encrypted content using said content key.

51. The secure hard drive of Claim 50 further comprising content playing means for receiving said decrypted digital content from said block decryption means and for generating an analog output signal.

52. The secure hard drive of Claim 50 further comprising chip identification (ID) means for providing a chip ID for said SOC, wherein said private key and a public key of said SOC is based on said chip ID.

53. The secure hard drive of Claim 50 wherein said SOC further includes controller means for performing buffer management and timing of read/write operations.

54. A system comprising the secure hard drive of Claim 53 and further comprising:

an external host; and

control interface means provides an interface between said controller means and said external host.

55. The secure hard drive of Claim 51 further comprising watermark detecting means that communicates with an output of said content playing means for determining whether said analog signal that is output by said content playing means contains a watermark.

56. The secure hard drive of Claim 50 wherein said magnetic storage means stores a content directory having content directory entries for said content.

57. The secure hard drive of Claim 56 wherein said public key decryption means performs digital signature verification of said content directory entry corresponding to said content that is selected for play.

58. The secure hard drive of Claim 56 wherein said content directory entries contain at least one of clear content counting means for specifying a portion of said corresponding content that is not encrypted, a content distributor identification (ID) field that identifies a content distributor supplying said corresponding content, a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback, a signature field for said content distributor supplying said corresponding content, a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said magnetic storing means, and a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said magnetic storing means.

59. The secure hard drive of Claim 50 wherein said content includes at least one of audio, video, and still pictures.

60. The system of Claim 54 further comprising:

distributed means for providing a distributed communications network; and

content distributor means for transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed means.

61. A method for distributing digital content, comprising:

(a) storing encrypted digital content and corresponding encrypted content keys on a storage medium;

(b) receiving one of said encrypted content keys from said storage medium;

(c) decrypting said encrypted content key using a private key to generate a content key;

(d) receiving said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium; and

(e) decrypting said encrypted content using said content key.

62. The method of Claim 61 wherein said storage medium is a magnetic storing medium.

63. The method of Claim 61 further comprising generating at least one of an analog output signal and a digital output signal based on said decrypted digital content.

64. The method of Claim 61 further comprising interfacing with an external host.

65. The method of Claim 63 further comprising determining whether said analog signal contains a watermark.

66. The method of Claim 61 further comprising storing a content directory having content directory entries for said content on said storage medium.

67. The method of Claim 66 further comprising performing digital signature verification of said content directory entry corresponding to said content that is selected for play.

68. The method of Claim 66 further comprising specifying a portion of said corresponding content that is not encrypted using a clean content field in at least one of said content directory.

69. The method of Claim 66 further comprising identifying a content distributor supplying said corresponding content using a content distributor identification (ID) field in at least one of said content directory entries.

70. The method of Claim 66 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storage medium.

71. The method of Claim 66 wherein at least one of said content directory entries includes a signature field for said content distributor supplying said corresponding content.

72. The method of Claim 66 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storing means.

73. The method of Claim 66 wherein at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in an encrypted content block stored on said storing means.

74. The method of Claim 61 wherein said content includes at least one of audio, video, and still pictures.

75. The method of Claim 64 further comprising:

providing a distributed communications network; and

transmitting encrypted content, an encrypted content key, and a content directory entry for a content selection from at least one content distributor to said secure hard drive via said external host and said distributed communications network.

76. The method of Claim 61 further comprising pre-storing encrypted content on said storage medium.

77. The method of Claim 61 further comprising performing steps (b), (c), (d) and (e) using a system on chip (SOC).